

AO 106 (Rev. 7/87) Affidavit for Search Warrant *

United States District Court

DISTRICT OF DELAWARE

In the Matter of the Search of

(Name, address or brief description of person, property or premises to be searched)

The premises located at**Wilmington, Delaware 19810****APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT****REDACTED****CASE NUMBER: 08-138M**I Michelle Carron Taylor being duly sworn depose and say:I am a(n) Special Agent, Federal Bureau of Investigation and have reason to believe
Official Titlethat ☐ on the person of or ☒ on the property or premises known as (name, description and/or location)**2114 Exton Drive, Wilmington, Delaware 19810 (as more fully described in Attachment A)**in the District of Delaware

there is now concealed a certain person or property, namely (describe the person or property to be seized)

See Attachment B**which is** (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)**evidence, fruits and instrumentalities of the unlawful transportation, receipt and possession of child pornography (as more fully described in Attachment B)**concerning a violation of Title 18 United States Code, Section(s) 2252 & 2252A.**The facts to support a finding of Probable Cause are as follows:****See Attached Affidavit**

Continued on the attached sheet and made a part hereof.

☒ Yes ☐ No

Reviewing AUSA: Edward J. McAndrew

Signature of Affiant

Michelle Carron Taylor, Special Agent
FBI

Sworn to before me, and subscribed in my presence

Date

8/8/08

at

Wilmington, Delaware

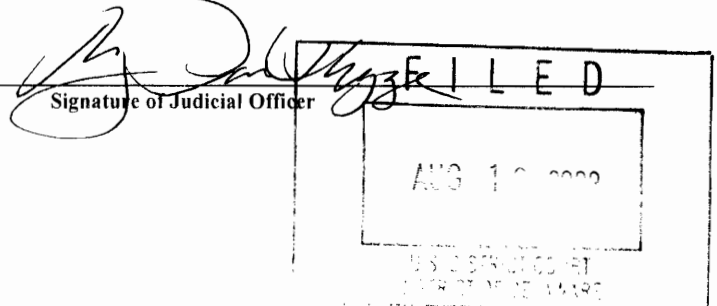
City and State

Mary Pat Thyne

United States Magistrate Judge

Name and Title of Judicial Officer

Signature of Judicial Officer



IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

IN THE MATTER OF THE)
SEARCH OF:)
THE PREMISES KNOWN AS)
Wilmington, Delaware 19810)

Case No.08-130M

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The location known as .

Wilmington, Delaware 19810 is identified as:

a two story, single family dwelling with a light yellow exterior. This house has a brown roof and maroon shutters. The number is posted on the mailbox in front of the house.



**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

IN THE MATTER OF THE)
SEARCH OF:)
THE PREMISES KNOWN AS) Case No.08- 138M
)
Wilmington, Delaware 19810)

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

- A. images of child pornography or child erotica and files containing images of such in any form wherever it may be stored or found including, but not limited to:
- i. any cellular telephone, personal digital assistant, computer, computer system and related peripherals; computer hardware; computer software; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, monitors, printers, external storage devices, routers, modems, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to computer passwords and data security devices and computer-related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;
 - ii. books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
 - iii. originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
 - iv. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

- B. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:
- i. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
 - ii. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
 - iii. Any and all records, documents, or materials, including any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;
 - iv. Any and all records, documents, or materials, including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256;
 - v. Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums, including CDs or DVDs;
- C. credit card information including but not limited to bills and payment records, including but not limited to records of internet access;
- D. records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;
- E. records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access,

and handwritten notes;

- F. Any and all adapters, chargers or other hardware items necessary to charge the battery, or to maintain the functioning of, any of the equipment described above.

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

| | | |
|----------------------------|---|------------------|
| IN THE MATTER OF THE |) | |
| SEARCH OF: |) | |
| THE PREMISES KNOWN AS |) | Case No.08- 138M |
| 2114 Exton Drive |) | |
| Wilmington, Delaware 19810 |) | |

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Michelle Carron Taylor, a Special Agent with the Federal Bureau of Investigation (FBI), Baltimore Division, Wilmington, Delaware Resident Agency, being duly sworn, depose and state as follows:

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI). I have been so employed since November 2005. My current duties include investigating federal crimes involving child sexual exploitation.
2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.
3. I am investigating the activities of Brian L. Briggs, or any other person, who used a computer connecting to the internet from a service and billing address of Wilmington, Delaware 19810 (the "SUBJECT PREMISES"). As will be shown below, there is probable cause to believe that someone using a computer at the SUBJECT PREMISES has transported, received and possessed child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. I am submitting this affidavit in support of a search warrant

authorizing a search of the SUBJECT PREMISES, which is more particularly described in Attachment A, and the seizure of the items more particularly described in Attachment B.

4. All information contained in this affidavit is either personally known to the affiant or has been related to the affiant by other Special Agents of the Federal Bureau of Investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, U.S.C. §§ 2252 and 2252A, are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors. 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of a minor engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce. 18 U.S.C. § 2252A(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when

such child pornography was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

- a. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
- b. “Child Pornography,” as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).
- c. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).
- d. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).
- e. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device

performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”

f. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock”

particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which preform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

k. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

l. An Internet Service Provider (ISP) is a commercial service that provides Internet connectivity to its subscribers. In addition to providing access to the Internet via telephone lines or other telecommunications lines/cables, ISPs may also provide Internet e-mail accounts and other services unique to each particular ISP such as Usenet (newsgroups) and chat/messaging functions. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, customer service information and other information, both in computer data format and in written record format.

m. A "server" is a centralized computer that provides services for other computers connected to it via a network. The computers that use the server's services are sometimes called "clients."

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

7. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

8. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

9. Child pornographers can transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With digital cameras the images can be transferred directly onto a computer. A computer can connect to another computer through the use of telephone, cable, or wireless connections. Electronic contact can be made to literally millions of computers around the world.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

11. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

12. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found

on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

13. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

14. A growing phenomenon on the Internet is peer to peer file sharing (P2P). P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting a search for files that are currently being shared on the network. Limewire, one type of P2P software, sets up its searches by keyword. The results of the keyword search are displayed to the user. The user

then selects file(s) from the results for download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file.

15. For example, a person interested in obtaining child pornographic images would open the P2P application on his/her computer and conduct a search for files using a term such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user selects from the results displayed of the file(s) he/she wants to download. The file is downloaded directly from the computer hosting the file. The downloaded file is stored in the area previously designated by the user. The downloaded file will remain there until moved or deleted.

16. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a Limewire user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. Often, however, a Limewire user downloading an image file receives the entire image from one computer.

17. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

18. Third party software is available to identify the IP address of the P2P computer sending the file and to identify if parts of the file came from one or more IP addresses. Such software monitors and logs Internet and local network traffic.

Google “Hello” Program

19. At all relevant times, Google’s “Hello” software program was an internet service that enabled users to trade image files easily, quickly, and relatively securely. Google Hello was shut down in or about June 2008.

20. The Hello program allowed traders to connect directly (peer-to-peer) to each other’s computers specifically for the purpose of sharing pictures. Movie files also could be shared. Since the connection was peer-to-peer, there was no limit to the number and size of files that could be shared. Once a connection was created, the individuals simply selected the files they wished to share. This could be an individual picture or video, or a folder containing thousands of pictures. While connected, the individuals also could engage in chat conversations. Thus, users could share pictures or videos and chat about them in real time as the images appeared on their computer monitors. All pictures and chat were encrypted during the transmission by the software. This overcame the traditional limitation of peer-to-peer software by facilitating both live chat and exchange of large volumes of files simultaneously.

21. As individuals used the Hello application, the program created a series of directories on the hard drive of the computer. These directories and their structure on the computer are used for organizing, recording and maintaining chat records, shared images, “friends lists” and “thumbnails” or reduced versions of the images that were transmitted or received. Each time the user joined a chat with another Hello user, the directory structure would

grow to accommodate the records of the chats with each new user. On newer computers that utilize the Microsoft Windows 2000 or Windows XP operating systems, these directories by default are found within the computer user's Documents and Settings directory.

22. Because this data was saved to the hard drive of the computer that was used to access the Hello application, the data would remain on the computer and be unaffected by the discontinuation of the Hello service.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

23. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems

and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

24. To fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

25. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, printer, modem, router, or any other computer hardware or software found at the SUBJECT PREMISES are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251 through 2256, and should all be seized as such.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

26. Affiant has been informed that FBI Supervisory Special Agent (SSA) James T. Clemente has worked in the Behavioral Analysis Unit of the FBI since 1998. SSA Clemente has been a special agent with the FBI since 1987. As a member of the Behavioral Analysis Unit,

SSA Clemente consults on child exploitation cases throughout the United States, South America, and certain European and African countries. Since 1998, he has received three Exceptional Performance Awards from the Department of Justice and a Superior Service Award from the FBI. In addition, he has received numerous letters of commendation from state, federal, and local law enforcement in connection with his work in the Behavioral Analysis Unit.

27. SSA Clemente's training has involved a significant number of specialized courses in the area of child exploitation, including, but not limited to the following: Innocent Images On-Line Sex Crimes Against Children; National Crimes Against Children; On-Line Sex Crimes Against Children; Clinical Forensic Psychology; Behavioral Analysis of Violent Crime; Missing and Exploited Children Seminar; Research Methodologies; MO, Ritual & Signature Advanced Seminar; and Criminology. In addition, he has mentored under, worked with, studied the articles of, and taught with Kenneth V. Lanning, a Supervisory Special Agent, FBI (retired as of October, 2000). SSA Lanning has over the past 27 years authored numerous articles on the topic of sexual victimization of children and behavioral analysis of child molesters. His work forms the basis of the behavioral analysis performed by the FBI in child exploitation cases.

28. SSA Clemente has assisted in the writing of numerous search warrant affidavits and has testified as an expert witness in federal court in the areas of child sex offender behavior, child sexual victimology and child pornography. He has given over 100 presentations and lectures to local, state and federal law enforcement agencies, prosecutors, and health care professionals throughout the United States on various topics related to child exploitation, including, but not limited to the following topics: Behavioral Analysis of Child Sex Crimes Offenders, On-Line Sex Crimes Against Children, and Equivocal Death Investigations.

29. As a member of the Behavioral Analysis Unit, SSA Clemente has analyzed and consulted on between one and two hundred child sexual exploitation and victimization cases a year. His analyses are based on all available evidence, including chat records, image collection analysis, collection themes, possession of erotica, possession of sexual paraphernalia, fantasy literature and writings, other relevant acts, and background information. The vast majority of the cases he has analyzed have involved either Preferential or Situational Sex Offenders. His role in these cases has varied as follows: analyzing investigative results for the purpose of making investigative suggestions, providing expert affidavits for search warrant applications, providing interview strategies for subjects and victims, consulting with local, state and federal prosecutors on trial strategies. In addition, SSA Clemente has interviewed between 80 and 100 offenders himself. A behavioral assessment is not a clinical diagnosis; rather, it is a law enforcement tool used to identify and predict offender behavior.

30. SSA Clemente advises of the following traits and characteristics that are generally found to exist and be true in cases involving individuals who collect child pornography:

- a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.
- b. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text

that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials.

BACKGROUND OF THE INVESTIGATION

31. On May 14, 2008, SA Jeffrey L. Coburn, of the Phoenix Division of the FBI, conducted an undercover session on the internet utilizing the publicly available Google "Hello" program.

32. During this undercover session, SA Coburn was contacted by an individual with the user-name "TomatoB," who sent SA Coburn twenty-eight images, some of which were child pornography.

33. One of the images that "TomatoB" sent to SA Coburn was named "0_16690500_1184632791.jpg." This image depicted a prepubescent girl approximately five or six years old, holding an erect adult male penis near her face.

34. During the transmission of the images from "TomatoB" to SA Coburn, they communicated with one another using the "Hello" program. During this chat session, "TomatoB" advised that his real name was Brian, he is twenty-two years old, and his Yahoo! user-id was "briggsy2111." Regarding his child pornography collection, "TomatoB" advised that he has a Dell laptop computer and another desktop computer and explained that his "desk top has all the main stuff and new things come in on the laptop." "TomatoB" further elaborated that he has images of children under thirteen years old engaged in sexual activity on his desktop computer at his house.

35. Also during the chat session, "TomatoB" advised that he has a "useless english

degree" and that he "maybe someday be a teacher." SA Coburn then queried "get to be by little girls then..?", to which "TomatoB" responded that would be a "fringe benefit" of being a teacher.

36. Also during the chat session, "TomatoB" advised that he had sexually touched a child "a few years back" when he "was eighteen years old and working at a camp" when he was "helping a kid put on her swim suit" and "got a great feel for the ass and chest."

37. Also during the session, "TomatoB" asked SA Coburn if "she" had any children, to which SA Coburn responded that "she" had an 13-year-old daughter. "TomatoB" asked SA Coburn if she was "active" with "her" daughter, and asked SA Coburn to transmit nude images of "her" daughter.

38. On May 19, 2008, SA Coburn served an administrative subpoena on Google, Inc, requesting subscriber information for the user-id "TomatoB."

39. On May 30, 2008, Google Inc. responded to the administrative subpoena with the following information:

User-ID: 4258911
Username: TomatoB
E-mail: mrb111122111@aol.com (all number '1's)
05/14/2008 07:52:07 PDST 72.94.230.4 on
05/14/2008 08:36:06 PDST 72.94.230.4 off

40. Using a publicly available software tool, SA Coburn conducted a whois lookup of the IP address 72.94.230.4, which showed that it resolved to the internet service provider Verizon Internet Services.

41. On June 4, 2008, an administrative subpoena was served upon Verizon for

subscriber information for the accounts that was using the IP address 72.94.230.4 at the dates/times the images of child pornography were transferred from "TomatoB" to SA Coburn.

42. On June 5, 2008, Verizon Internet Services advised SA Coburn that for all of the requested dates/times, the above IP address was assigned to an internet service account subscribed to by: Cinda J. Crane, [redacted] Wilmington, Delaware 19810 (*i.e.*, the SUBJECT PREMISES), phone numbers [redacted], Verizon User-ID's "cranecj" and "jbriggs13."

43. On or about June 20, 2008, using the publicly available website www.lexisnexis.com, a law enforcement officer determined that the address Wilmington, DE 19810 lists the following household members: Brian L. Briggs, Cinda J. Crane, Janet M. Briggs, and John Edward Briggs.

44. On or about July 8, 2008, Your affiant determined that the Delaware Justice Information System (DELJIS) indicated that John Edward Briggs' driver's license lists his current address as [redacted] Wilmington, Delaware 19810, which is the same as SUBJECT PREMISES.

45. On August 2, 2008, a law enforcement officer conducted visual surveillance of the SUBJECT PREMISES, which is pictured in Attachment A and which may be described as a two-story, single family dwelling with light yellow siding. This house has a brown roof and maroon shutters. The number [redacted] is posted on the mailbox in front of this house. Parked in the driveway of this address was a dark green 2005 Honda Odyssey with Delaware plates PC110365 and a grey 2003 Honda Accord with Delaware plates 319438; both of which are registered to Cinda Crane and John Briggs, at the SUBJECT PREMISES.

46. On August 2, 2008, a representative of the United States Postal Service confirmed that John Briggs receives mail at SUBJECT PREMISES.

47. On August 6, 2008, law enforcement agents executed a federal search warrant at Brian L. Briggs' Wilmington residence. Briggs, his father and his mother were present when agents entered the residence.

48. Pursuant to the search warrant, law enforcement agents seized various pieces of computer equipment, including a laptop, a thumb drive, a number of other computers and various computer equipment and media. Law enforcement officers saw, but did not take, a cell phone that appeared to be a Motorola brand, which was located on a dresser in the residence.

49. A preview search of the thumb drive, which Brian L. Briggs identified as his own, was found to contain over 100 images of suspected child pornography. For example, one image depicts a prepubescent girl, approximately 10-11 years old, engaged in oral sex with a naked adult male. Another image depicts a naked female, approximately 13 years old, masturbating while she performs oral sex on a naked adult male.

50. Brian L. Briggs consented to an interview with law enforcement officers. During the course of the interview, Brian L. Briggs was shown two of the images that UC-1 received from "TomatoB" – both of which Briggs admitted transmitting during the Google Hello session. One of these images depicts a prepubescent girl who appears to be under age five grasping an adult male penis. Briggs also was shown a transcript of his May 14, 2008 Google Hello chat with UC-1, in which he acknowledged engaging.

51. Brian L. Briggs also provided a written statement admitting:

I started looking at illegal under-aged pictures of girls in the last few years. At the time these images were interesting to me. I used a chat site called literotica.com to meet other like minded people, and we traded pictures.

52. Brian L. Briggs also stated that he is a camp counselor for the Friends Central School summer camp program located in Wynnewood, Pennsylvania. During the school year, he works in the after-school program at the same school. His duties include escorting children aged 6-12 to various activities and monitoring them as they change clothes.

53. Since the August 6, 2008 search and interview of Brian Briggs, law enforcement agents have interviewed co-workers and administrators at the Friends Central School.

54. On August 8, 2008, law enforcement officers interviewed one co-worker, whose two minor children Brian Briggs babysat on the evening of August 5, 2008 (the night before the residential search).

55. This co-worker informed the agents that Brian Briggs had a cell phone capable of taking digital photographs, which he brought to the summer camp. She believed the cell phone to be a Motorola Razr. She and/or other co-workers had witnessed the phone being used to take digital photographs of adults at one of the co-workers' swimming pool.

56. Based on my training and experience, and based on conversations that I have had with other law enforcement agents who conduct high-tech investigations, I know that many cell phones – including the Motorola Razr – have the capability to take and to store digital photographs and/or videos. These cell phones also can be used as mobile storage devices, and can be used to transfer electronic files containing digital photographs and videos to and from other computer equipment

CONCLUSION


57. Based on the above information, there is probable cause to believe that the SUBJECT PREMISES contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A.

58. In consideration of the foregoing, Your affiant respectfully requests that this Court issue a warrant to search the SUBJECT PREMISES, as more particularly described in Attachment A, and to seize the items specified in Attachment B.

Respectfully submitted,


SA Michelle Carron Taylor, FBI

Sworn and subscribed before me
this 8 day of August 2008


Honorable Mary Pat Thyng
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

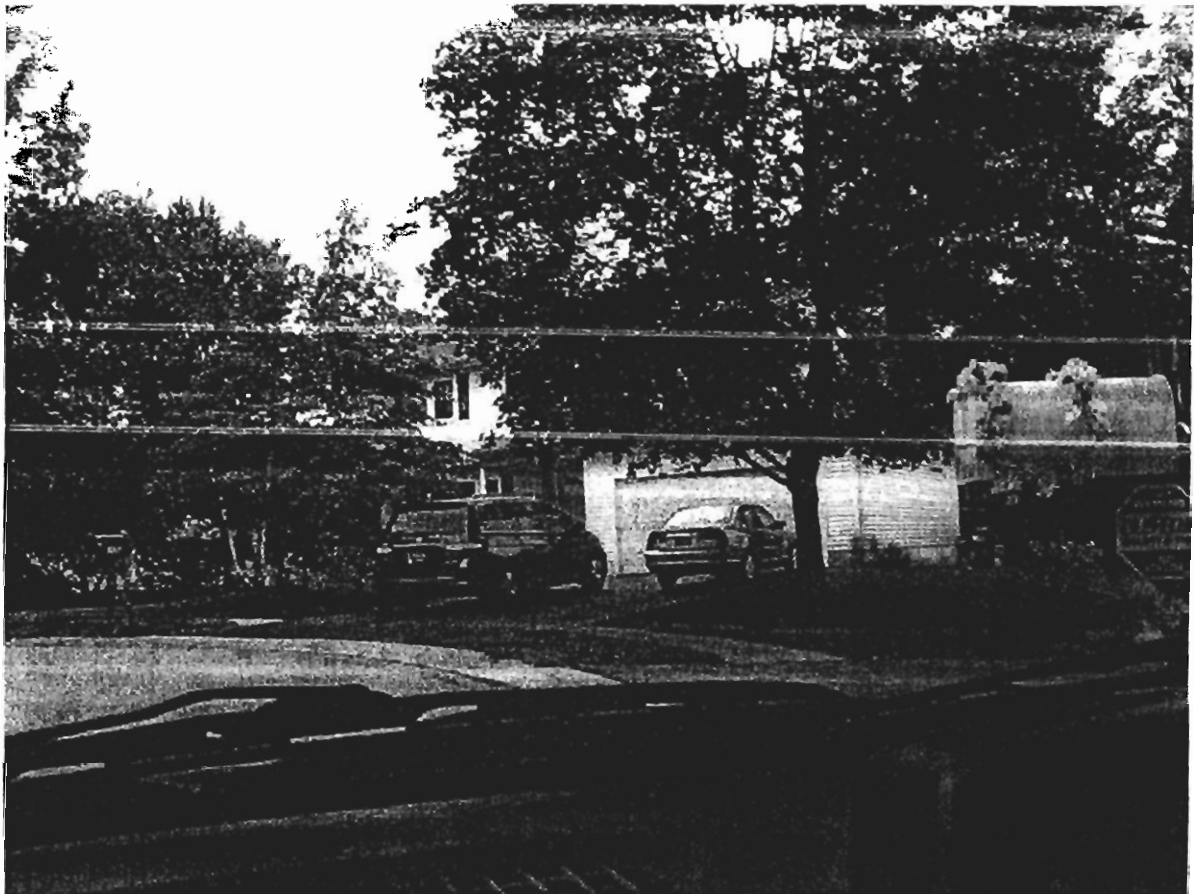
IN THE MATTER OF THE)
 SEARCH OF:)
 THE PREMISES KNOWN AS) Case No.08-
 2114 Exton Drive)
 Wilmington, Delaware 19810)

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The location known as : Wilmington, Delaware 19810 is identified as:

a two story, single family dwelling with a light yellow exterior. This house has a brown roof and maroon shutters. The number _____ is posted on the mailbox in front of the house.



**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

| | | |
|----------------------------|---|-------------|
| IN THE MATTER OF THE |) | |
| SEARCH OF: |) | |
| THE PREMISES KNOWN AS |) | Case No.08- |
| 2114 Exton Drive |) | |
| Wilmington, Delaware 19810 |) | |

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

- A. images of child pornography or child erotica and files containing images of such in any form wherever it may be stored or found including, but not limited to:
- i. any cellular telephone, personal digital assistant, computer, computer system and related peripherals; computer hardware; computer software; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, monitors, printers, external storage devices, routers, modems, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to computer passwords and data security devices and computer-related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;
 - ii. books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
 - iii. originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
 - iv. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

- B. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:
- i. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
 - ii. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
 - iii. Any and all records, documents, or materials, including any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;
 - iv. Any and all records, documents, or materials, including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256;
 - v. Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums, including CDs or DVDs;
- C. credit card information including but not limited to bills and payment records, including but not limited to records of internet access;
- D. records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;
- E. records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access,

and handwritten notes;

- F. Any and all adapters, chargers or other hardware items necessary to charge the battery, or to maintain the functioning of, any of the equipment described above.